AMENDMENTS TO CLAIMS

Claim 1 (original): A system for secure transmission of protected content, the system comprising:

a security server;

a recipient module; and

a secure communication channel for supporting communication between said security server and said recipient module,

wherein, in a first mode of operation, the recipient module receives a first key in a multiple key hierarchy via said secure channel, and

in a second mode of operation, the recipient module receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said recipient module being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said recipient module only being capable of accessing the protected content with said decrypted key.

Claim 2 (original): The system of claim 1, wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said recipient module is entitled to access the protected content and said VEMM being prepared by said security server.

Claim 3 (original): The system of claim 2, wherein said access criteria reference for each item of protected content is associated with a separate access key.

Claim 4 (original): The system of claim 2, wherein said encrypted key further comprises an encrypted control word.

Claim 5 (original): The system of claim 4, wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said recipient module and said VECM being prepared by said security server.

Claim 6 (original): The system of claim 5, wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said recipient module, and such that said recipient module is capable of decrypting said subscriber key.

Claim 7 (original): The system of claim 6, wherein said recipient module further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel.

Claim 8 (original): The system of claim 7, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

Claim 9 (original): The system of claim 8, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

Claim 10 (original): The system of claim 9, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 11 (original): The system of claim 7, wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret.

Claim 12 (original): The system of claim 7, further comprising a head-end for transmitting the protected content.

Claim 13 (original): The system of claim 12, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

Claim 14 (original): The system of claim 13, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

Claim 15 (original): The system of claim 14, wherein said head-end also sends said ECM to said recipient module.

Claim 16 (original): The system of claim 14, wherein a different VEMM is transmitted periodically.

Claim 17 (original): The system of claim 16, wherein a different VEMM is transmitted if said recipient module is off-line for at least a predetermined period of time.

Claim 18 (original): The system of claim 14, further comprising a plurality of recipient modules, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules.

Claim 19 (original): The system of claim 14, further comprising a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server.

Claim 20 (original): The system of claim 19, wherein said subscriber key at said remote renewable security element is capable of being renewed.

Claim 21 (original): The system of claim 19, wherein said remote renewable security element further comprises a hardware component and a software component.

Claim 22 (original): The system of claim 21, wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said recipient module.

Claim 23 (original): The system of claim 21, wherein said hardware component encrypts said access key and said control word.

Claim 24 (original): The system of claim 19, further comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 25 (original): The system of claim 19, wherein a plurality of said remote renewable security elements is controlled by said security server.

Claim 26 (original): The system of claim 25, wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key.

Claim 27 (original): The system of claim 26, wherein said security server generates said access key in an encrypted form as an encrypted access key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key.

Claim 28 (original): The system of claim 19, wherein said recipient module comprises a set-top box.

Claim 29 (original): A system for secure transmission of protected content, comprising:

(a) a remote renewable security element for encrypting a plurality of keys in a multiple key hierarchy; and

(b) a recipient module for receiving the protected content and said plurality of encrypted keys, said recipient module comprising a secret for decrypting at least one encrypted key to form a first decrypted key, said first decrypted key being required to decrypt at least one additional key in said multiple key hierarchy, wherein said recipient module is only capable of accessing the

protected content with said at least one additional decrypted key in said multiple key hierarchy.

Claim 30 (original): The system of claim 29, wherein said first encrypted key is only capable of being decrypted according to said secret.

Claim 31 (original): The system of claim 30, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

Claim 32 (original): The system of claim 31, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

Claim 33 (original): The system of claim 32, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

Claim 34 (original): The system of claim 33, comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

Claim 35 (original): The system of claim 29, wherein at least one of said keys in said multiple key hierarchy at said remote renewable security element is capable of being renewed.

Claim 36 (original): The system of claim 29, wherein said remote renewable security element comprises at least one encryption mechanism.

Claim 37 (original): The system of claim 36, further comprising a security server for receiving said first encrypted key encrypted with said secret and also for

receiving said first key as an unencrypted key, such that said secret is not accessible to said security server or to said remote renewable security element.

Claim 38 (original): The system of claim 37, further comprising a head-end for broadcasting the protected content.

Claim 39 (original): The system of claim 38, wherein said head-end transmits an access criteria reference to said security server, and wherein said security server packages said access criteria reference at least with said first encrypted key for transmitting to said recipient module.

Claim 40 (original): The system of claim 39, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

Claim 41 (original): The system of claim 40, wherein said security server constructs a VEMM from said EMM and sends said VEMM to said recipient module.

Claim 42 (original): The system of claim 41, wherein a different VEMM is transmitted periodically.

Claim 43 (original): The system of claim 41, wherein said security server receives an access key, encrypted with said first key, from said remote renewable security element, and wherein said security server sends said encrypted access key to said recipient module.

Claim 44 (original): The system of claim 43, wherein said access key is not sufficient to access the protected content, and wherein said security server receives a control word, encrypted with said access key, from said remote renewable security element, and wherein said security server sends said encrypted control

word to said recipient module, said control word being sufficient for said recipient module to access the protected content.

Claim 45 (original): The system of claim 44, wherein said security server receives said control word from said head-end.

Claim 46 (original): The system of claim 44, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

Claim 47 (original): The system of claim 46, wherein said head-end also sends said ECM to said recipient module.

Claim 48 (original): The system of claim 47, further comprising a set-top box for receiving the protected content, said set-top box comprising a smart card located at said set-top box, said set-top box receiving said ECM and said EMM from said head-end if said set-top box is authorized to access the protected content, such that said set-top box is not required to be in communication with said security server.

Claim 49 (original): The system of claim 39, wherein said recipient module comprises a set-top box.

Claim 50 (original): The system of claim 49, wherein each access criteria reference is associated with a different access key.

Claim 51 (original): A server for supporting secure transmission of protected content to a recipient module, the protected content being broadcast by a head-end, the head-end providing an access criteria reference and a control word for accessing the protected content, the server comprising:

(a) a remote renewable security element;

(b) an entitlement message generator; and

(c) a control word message generator;

wherein said entitlement message generator receives the access criteria reference from the head-end and queries said remote renewable security element to determine whether the recipient module is entitled to receive the protected content, such that if the recipient module is entitled to receive the protected content, said entitlement message generator generates a VEMM comprising an encrypted access key and the access criteria reference; and

wherein if the recipient module is entitled to receive the protected content, said control word message generator receives the control word from the head-end and generates a VECM comprising an encrypted control word, such that the recipient module cannot access the protected content without said VEMM and said VECM.

Claim 52 (original): A server for supporting secure transmission of protected content to a recipient module, the server comprising:

(a) a remote renewable security element for determining whether the recipient module has at least one entitlement to the protected content;

(b) a VEMM generator for generating a first message containing a first key, said VEMM generator only generating said first message if the recipient module has said at least one entitlement; and

(c) a VECM generator for generating a second message containing a second key, said second key being encrypted with said first key, wherein the protected content is only accessible according to said second key.

Claim 53 (original): The server of claim 52, wherein the recipient module comprises a secret and said first key is encrypted, and wherein access to said first key by the recipient module is at least partially determined according to said secret.

Claim 54 (original): The server of claim 53, wherein the recipient module receives a subscriber key encrypted with said secret from the server, and wherein said first key is encrypted with said subscriber key.

Claim 55 (original): The server of claim 52, wherein said remote renewable security element further comprises a hardware component for encrypting said second key with said first key, and a software component for determining said entitlement.

Claim 56 (currently amended): A method for transmitting protected content by a broadcaster for being accessed by a subscriber, comprising:

providing a recipient module for the subscriber, said recipient module comprising a unique secret;

determining at least one access permission for said recipient module;

generating an access key to form an access message according to said access permission;

encrypting said access key to form an encrypted key, such that said secret is required to decrypt said encrypted key;

encrypting a control word with said access key to form an encrypted control word; and

transmitting said encrypted key and said control word to said recipient module,

wherein said recipient module requires at least said control word to access the protected content.

Claim 57 (original): The method of claim 56, wherein each subscriber has an associated subscriber key, and wherein the broadcaster receives said subscriber key and said subscriber key encrypted with said secret to form an encrypted subscriber key, such that the broadcaster transmits said encrypted subscriber key to said recipient module as at least a portion of said encrypted key.

Claim 58 (original): The method of claim 57, wherein said determining at least one access permission for said recipient module comprises determining an entitlement to the protected content by the subscriber.

Claim 59 (original): The method of claim 58, wherein said encrypted access key is encrypted with said subscriber key.

Claim 60 (original): The method of claim 59, wherein said encrypting said key with said secret to form said encrypted key further comprises constructing a VEMM, said VEMM comprising said encrypted subscriber key, said encrypted access key and at least one access criteria reference.

Claim 61 (original): The method of claim 60, wherein said encrypted control word is sent as part of a VECM, said VECM further comprising said at least one access criteria reference and a crypto-period index.

Claim 62 (original): The method of claim 61, further comprising:

receiving said VEMM by said recipient module;

obtaining said access key from said VEMM with said secret and said subscriber key;

receiving said VECM by said recipient module;

obtaining said control word from said VECM with said access key; and

accessing the protected content with said control word.

Claim 63 (new): The system of claim 2 and wherein said VEMM is sent upon request by said recipient module.

Claim 64 (new): The system of claim 63 and wherein said request includes an access criteria reference.

Claim 65 (new): The system of claim 63 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 66 (new): The system of claim 5 and wherein said secure communication channel further comprises a subscriber key, such that said first key

is encrypted with said subscriber key for being transmitted to said recipient module, and such that only said recipient module is capable of decrypting said subscriber key.

Claim 67 (new): The system of claim 1 and wherein at least one of said security server and said secure communication channel is implemented with redundant components.

Claim 68 (new): The system of claim 41 and wherein said VEMM is sent upon request by said recipient module.

Claim 69 (new): The system of claim 68 and wherein said request includes an access criteria reference.

Claim 70 (new): The system of claim 68 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 71 (new): The system of claim 29 and wherein said remote renewable security element is implemented with redundant components.

Claim 72 (new): The server of claim 51 and wherein said VEMM is generated upon request by said recipient module.

Claim 73 (new): The server of claim 72 and wherein said request includes an access criteria reference.

Claim 74 (new): The server of claim 72 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 75 (new): The server of claim 51 and wherein at least one of said remote renewable security element, said entitlement message generator, and said control word message generator is implemented with redundant components.

Claim 76 (new): The server of claim 52 and wherein said VEMM generator generates said first message upon request by said recipient module.

Claim 77 (new): The server of claim 76 and wherein said request includes an access criteria reference.

Claim 78 (new): The server of claim 76 and wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user.

Claim 79 (new): The server of claim 52 and wherein at least one of said remote renewable security element, said VEMM generator, and said VECM generator is implemented with redundant components.

Claim 80 (new): The method of claim 60 and wherein said VEMM is constructed upon request by said recipient module.

Claim 81 (new): The method of claim 80 and wherein said request includes an access criteria reference.

Claim 82 (new): The method of claim 80 and wherein said request is sent in response to an impulse pay per view (IPPV) request by a user.